



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/612,142 | 07/07/2000 | Ronald Glen Feigen | IRI05275 | 7805 |

22863 7590 06/15/2004

MOTOROLA, INC.
CORPORATE LAW DEPARTMENT - #56-238
3102 NORTH 56TH STREET
PHOENIX, AZ 85018

EXAMINER

NALVEN, ANDREW L

| ART UNIT | PAPER NUMBER |
|----------|--------------|
|----------|--------------|

2134

DATE MAILED: 06/15/2004

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/612,142

Applicant(s)

FEIGEN ET AL.

Examiner

Andrew L Nalven

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 July 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-18 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-18 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claim 1-4, 6-10, 12-13, and 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Field et al US Patent No. 6,253,324 in view of Moskowitz et al US Patent No. 5,822,432. Field discloses a system for server verification of requesting clients and Moskowitz discloses a method for random key generation and application for digital watermarks.
5. With regards to claims 1, 8-9, and 16-17; Field teaches the determining of memory range information identifying a range of memory space within the remote unit having data to be hashed by the hashing function (Field, Figure 3 Items 204 and 206

Art Unit: 2134

and column 6 line 39 – column 7 line 40, column 7 lines 54-61) and delivering memory range information to the remote unit for use by the remote unit in performing a hashing operation (Field, column 7 lines 35-40, column 7 lines 54-61). Field's fails to teach the creation of a random number and determining position information indicative of a position within a data stream to be generated within the remote unit at which the random value it to be located. Moskowitz teaches the generating of a random value (Moskowitz, column 3 lines 24-27), the determining position information indicative of a position within a data stream to be generated within the remote unit at which the random value it to be located (Moskowitz, column 3 lines 24-30), and the delivering of the random value and position information to the remote unit (Moskowitz, column 3 lines 42-45). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Moskowitz's position determining method with Field's verification system because it offers the advantage of making it impossible for an unauthorized third party from acquiring the random value that is positioned with the data stream (Moskowitz, column 1 lines 39-45).

6. With regards to claims 2, 12, and 15, Field as modified further teaches the receiving of a hash value from the remote unit in which the hash value is a result of the hashing operation performed within the remote unit based upon the random value, memory range information, and position information delivered to the remote unit (Field, column 8 lines 6-42).

7. With regards to claims 3 and 13, Field as modified teaches the comparing of the hash value received from the remote unit to a hash value generated outside the remote unit (Field, column 8 lines 6-42).

8. With regards to claim 4, Field as modified teaches the hash value being generated outside the remote unit within a communication unit that is a replica of the remote unit by showing identical storage of data (Field, column 8 lines 6-12).

9. With regards to claim 5, Field as modified teaches the hash value generated outside the remote unit is a result of a hashing operation based upon the random value, memory range information, and position information (Field, column 7 lines 31-40).

10. With regards to claim 6, Field as modified teaches the steps of generating, determining memory range information, and position information is performed in a location different from the remote unit (Field, column 6 line 39 – column 7 line 40).

11. With regards to claim 7, Field as modified teaches a computer readable medium having program instructions stored thereon for use in implementing the method steps (Field, column 6 line 39 – column 7 line 40, column 8 lines 6-42).

12. With regards to claim 10, Field as modified teaches the transmitter transmitting the interrogation message to the remote unit via a communications network (Field, column 4 lines 17-44).

13. Claims 5 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Field et al US Patent No. 6,253,324 and Moskowitz et al US Patent No. 5,822,432, as

Art Unit: 2134

applied to claims 3 and 8 above, and in further view of Reeds III et al US Patent No 5,153,919.

14. With regards to claim 5, Field as modified fails to teach the hashing operation being based upon the random value, memory range, and position information. Reeds teaches the hash value generated outside the remote unit is a result of a hashing operation based upon the random value, memory range information, and position information (Reeds, column 5 lines 25-55, column 10 lines 3-5). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Reeds' method of hashing with Field as modified because it offers the advantage of a simple method of creating a signature for a block of data that can be easily carried out by a basic conventional processor because only simple operations are needed to complete the function (Reeds, column 5 line 65 – column 6 line 2).

15. With regards to claim 11, Reeds teaches a local memory storing information representative of the information that should be stored in the remote unit (Field, column 5 lines 16-25) and a hash unit for performing a hashing operation on information stored within the local memory to generate a control value (Field, column 7 lines 17-40). Field as modified fails to teach the hashing operation being based upon the random value, memory range, and position information. Reeds teaches the hash value generated outside the remote unit is a result of a hashing operation based upon the random value, memory range information, and position information (Reeds, column 5 lines 25-55, column 10 lines 3-5). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Reeds' method of hashing with Field as

Art Unit: 2134

modified because it offers the advantage of a simple method of creating a signature for a block of data that can be easily carried out by a basic conventional processor because only simple operations are needed to complete the function (Reeds, column 5 line 65 – column 6 line 2).

16. Claims 14 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Field et al US Patent No. 6,253,324 and Moskowitz et al US Patent No. 5,822,432, as applied to claims 8 and 15 above, in further view of Leighton et al US Patent No 5,432,852. Field as modified fails to teach a selection unit for selecting a hashing algorithm from a plurality of hashing algorithms. Leighton teaches selecting a hashing algorithm from a plurality of hashing algorithms for use by the remote unit and means for indicating the selected hashing algorithm to the remote unit (Leighton, column 14 lines 60-63). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Leighton's method of picking from a plurality of hashing algorithms with Field as modified because it makes it harder for an attacker to crack the hashing algorithm (Leighton, column 14 line 63 – column 15 line 7).

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

18. Trostle et al US Patent No 5,919,257 teaches a network workstation intrusion detection system that uses hashes to detect intrusions.

Art Unit: 2134


19. Lovelace et al US Patent No 6,263,431 teaches an operating system bootstrap security mechanism.


20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 703 305 8407. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven




MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137